



NETROPY[®] TRAFFIC GENERATION:

RFC 2544

USER'S GUIDE

Version 2.0



APPOSITE
— TECHNOLOGIES

Netropy® Traffic Generation RFC 2544 User's Guide

Revision 2a, March 2024

Apposite® Technologies LLC

4223 Glencoe Ave, Suite B121
Marina Del Rey, CA 90292 USA
1.310.477.9955
info@apposite-tech.com
www.apposite-tech.com

Copyright ©2005-2024 Apposite Technologies LLC. All rights reserved. Apposite, Linktropy, and Netropy Network Emulators and Traffic Generations are registered trademarks of Apposite Technologies LLC. The Apposite logo and "WAN Emulation Made Easy" are trademarks of Apposite Technologies LLC. Android and the Google Play logo are trademarks of Google Inc.

Part No. DOC-UG-NTG-RFC-2a

CONTENTS

- Contents 3
- 1 Overview 5
 - 1.1 Netropy Traffic Generation Configuration 5
 - 1.2 RFC 2544 Operation 5
- 2 Installation and Set-Up 7
 - 2.1 Preparation 7
 - 2.2 Hardware Installation 7
 - 2.3 IP Address Configuration via the Netropy GUI 7
 - 2.4 IP Address Configuration via the Serial Console 8
- 3 Configuration 9
 - 3.1 RFC 2544 9
 - 3.2 Throughput Test 9
 - 3.3 Latency Test 10
 - 3.4 Frame Loss Test 10
 - 3.5 Back-to-Back Test 10
- 4 Ports 11
 - 4.1 Overview of Ports 11
 - 4.1.1 Port Reset 11
- 5 Test Beds 13
 - 5.1 Overview of Test Beds 13
 - 5.2 Configuring Test Beds 13
- 6 Test Bed: Port Reservation 15
 - 6.1 Post Reservation Overview 15
 - 6.2 Adding Ports 15
 - 6.3 Removing Ports 15
- 7 Test Bed: Traffic Configuration 17
 - 7.1 Transmitter Configuration 17
 - 7.1.1 Port 18
 - 7.1.2 Port Speed 18
 - 7.1.3 Transmitter IP 18

7.1.4	Clients.....	18
7.1.5	Transmitter MAC	19
7.1.6	Dest MAC Address.....	19
7.1.7	External Gateway	20
7.2	Receiver Configuration	20
7.2.1	Port.....	21
7.2.2	Port Speed	21
7.2.3	Receiver IP.....	22
7.2.4	Receiver MAC.....	22
7.2.5	Dest MAC Address.....	22
7.2.6	External Gateway	22
8	Test Bed: Test Configuration	24
8.1	Test Configuration Overview	24
8.2	Test Configurations.....	25
8.2.1	Tx Custom Packets Size.....	25
8.2.2	Tx Packet Size	25
8.2.3	Number of Iterations.....	25
8.2.4	Iteration Duration(sec)	26
8.2.5	Bandwidth Order	26
9	Test Bed: Protocol Segment	27
9.1	Protocol Segment Overview	27
9.2	Adding Streams.....	27
9.3	Configuring Streams	28
10	Test Bed: Summary	29
10.1	Summary of Transmitter Configuration	29
10.2	Summary of Receiver Configuration	29
11	Statistics.....	31
11.1	Aggregate Statistics	31
11.2	Test Statistics	34
11.3	Offline Analyzer.....	35
11.4	Definitions: Statistics.....	38
12	Test Settings	40
12.1	Play/Pause/Stop	40
12.2	Clear Statistics	40
12.3	Start Packet Capture	41

13	Logs.....	42
	13.1 Logs Overview	42
	13.2 Managing Logs.....	42
	13.3 Log Files.....	43
14	Administration.....	44
	14.1 User Settings	44
	14.2 Port Settings.....	45
	14.3 Capture Settings.....	46
	14.4 License Settings.....	46
	14.5 Update Software Settings.....	47
	14.6 Advanced Settings	47
	14.7 Time Zone.....	48
	14.8 Signature	48
	14.9 DNS Queries File	49
15	Command Line Interface	50
	15.1 CLI Help	50
	15.2 CLI Top Level Commands	50
	15.3 RADIUS Management Commands	52
	15.4 LDAP Management Commands	52
16	Security	54
	16.1 Users and Passwords	54
17	Apposite Support.....	55
	17.1 Registration	55
	17.2 Customer Support.....	55
	Appendix A: Apposite End User License Agreement.....	57

1 OVERVIEW

Apposite Technologies would like to thank you for purchasing the Apposite Technologies' Netropy Traffic Generation RFC 2544. This User's Guide is intended to describe the proper installation, configuration, and operation of this product. Please reference the *Quick Start Guide* and *Hardware Guide* for additional information. The Quick Start Guide may be used to facilitate initial configuration and the Hardware Guide to outline the specific hardware components for each model.

1.1 Netropy Traffic Generation Configuration

The Netropy Traffic Generation must be configured through the browser-based Graphical User Interface (GUI) or using the CLI. The recommended browser is Google Chrome using HTTP or HTTPS.

1.2 RFC 2544 Operation

The configuration and use of the RFC 2544 requires the following configuration steps accessed using the system's GUI:

1. **Open the GUI**
Connect to the Netropy Traffic Generation using the default IP/Hostname assigned. Log in using your user account credentials.
2. **Reserve Ports**
Reserve the specified quantity of ports you will need for your test.
3. **Create Test Bed**
Name and select RFC 2544 to configure a new test bed.
4. **Add Ports**
Add the specified ports you need to the test.
5. **Configure Traffic**
Configure the transmitter and receiver settings.
6. **Configure the Test**
Select the specific tests you would like to conduct and then configure each test selection.
7. **Adjust the Protocol Segment**
Adjust the configuration settings for the protocol segment.

8. **Review the Summary**

Verify the Test Bed configuration.

9. **Start the Test**

Click the "Start Test" button to begin capturing data on the test bed.

10. **Evaluate Results and Logs**

View the graphs and statistics to analyze and evaluate the test results. Download any logs and reports.

11. **Adjust Configuration**

Alter the configuration after the initial test. This can be conducted to analyze various configurations and settings. All previous configuration steps from 4 to 7 can be adjusted on the same test bed.

2 INSTALLATION AND SET-UP

To configure and operate the Netropy Traffic Generation RFC 2544 through its browser-based GUI, the dedicated Ethernet management port must first be configured with an appropriate IP address and subnet mask. For convenience, the MGMT interface comes pre-configured with an IP address of 10.0.0.10 and is accessible from a directly connected host on the 10.0.0.0/255.0.0.0 subnet. The IP address and subnet mask of the MGMT interface can be changed through the GUI by an account with administrator privileges or by using the CLI.

2.1 Preparation

Management of the Netropy Traffic Generation device through the GUI requires a PC running an up-to-date web browser.

Initial configuration of the management interface requires:

- ▶ a PC running a supported web browser that can be configured and placed on the 10.0.0.0/255.0.0.0 network.

2.2 Hardware Installation

The Netropy Traffic Generation appliance is designed for installation in a standard 19" rack. Refer to the *Hardware Guide* for your specific model for rack-mount installation instructions.

Plug either one or two standard power cords into the Netropy Traffic Generation device, depending on your model, and turn on the power. Either a U.S. standard or a U.S. Y-power cable will be supplied with each unit. The system will be available for use within 1-4 minutes.

2.3 IP Address Configuration via the Netropy GUI

To configure the MGMT interface using the Netropy Traffic Generation GUI:

- 1 Configure a PC running a supported web browser with the IP address 10.0.0.2 or another address on the 10.0.0.0/255.0.0.0 subnet.
- 2 Connect an Ethernet cable between the PC and the MGMT port on the front of the Netropy Traffic Generation.

- ③ Open the browser on the PC and enter <http://10.0.0.10> in the address bar.
- ④ Review the End User License Agreement. The Netropy Traffic Generation GUI will be displayed once the License Agreement is accepted.
- ⑤ Log in using the username “admin@apposite-tech.com” and password “admin” to access the administrator portal.
- ⑥ Click on IP management in the top right corner and select change IP. Enter your network settings and select “Apply” to change these settings.
- ⑦ After the management interface has been configured, use the Ethernet cable to connect the MGMT port of the Netropy Traffic Generation to the management network.

2.4 IP Address Configuration via the Serial Console

- ① Using the provided RJ45 to DB9 cable, connect the serial port of a PC running terminal emulation software to the CONSOLE port of the Netropy. Set the serial port parameters to 9600 baud, 8 bits, no parity, 1 stop bit, and disable flow control. For more details on connecting to the serial console, see the Hardware Guide for your specific model.
- ② Press [ENTER] to display a login prompt. At the prompt, log in as “admin”, password is “admin”.

```
ntg login: admin
```

- ③ Use the following commands to set the IP address, netmask, and default gateway of the Netropy management interface:

```
[ntg]> mgmt set gw <default-gateway>
```

```
[ntg]> mgmt set addr <ip-address> netmask <mask>
```

IP addresses and subnet masks are entered in dotted-decimal format. For example:

```
[ntg]> mgmt set addr 192.168.1.1 netmask 255.255.255.0
```

- ④ Once the management interface has been configured, use an Ethernet cable to connect the MGMT port of the Netropy to the management network. Open a browser and enter the IP address of the MGMT interface in the address bar. The Netropy End User License Agreement will be displayed.
- ⑤ Review the License Agreement. The Netropy GUI will be displayed once the License Agreement is accepted.
- ⑥ Log in using username “admin” password “admin”.

3 CONFIGURATION

To enable efficient configuration of the Netropy RFC 2544 system, it is best to develop a fundamental understanding of some basic concepts and terminology.

3.1 RFC 2544

Request for comment (RFC) 2544 is a benchmarking methodology created in 1999 for testing and measuring the performance of network devices. By providing a common language and set of procedures for network engineers, RFC 2544 delivers standardized performance results that enable users to easily compare devices across different vendors.

The RFC includes 6 subtests that are designed to evaluate how a device will act in real-world scenarios. These tests are considered out-of-service, meaning the real network traffic must be stopped so that the tester can generate traffic with specific characteristics. These six subtests include the following:

- ▶ Throughput
- ▶ Latency
- ▶ Frame Loss
- ▶ Back-to-Back Frames (Burstability)
- ▶ System Reset
- ▶ System Recovery

As outlined in the RFC document, the ideal way to implement this series of tests is to use test equipment with both transmitting and receiving ports.

3.2 Throughput Test

The throughput test determines the maximum throughput that you can achieve without any packet loss. In an automated fashion, RFC 2544 will find the maximum throughput for a multitude of frame sizes from small to large packets. This value seeking test then gradually reduces throughput until zero packet loss is observed.

3.3 Latency Test

Latency is the time it takes a packet to travel from a source to a destination i.e. client to server, or test equipment to DUT. RFC 2544 measures latency by time stamping a test frame, transmitting it through the network and then checking the time stamp when the frame is received.

3.4 Frame Loss Test

Frame loss is the percentage of frames that were successfully transmitted from the source but were never received at the destination. RFC 2544 starts with a selected frame size and runs at 100% line rate for a specified duration. It steps down by 10% increments and records the results then repeats the tests with different frame sizes.

3.5 Back-to-Back Test

The back-to-back test characterizes the ability for the device under test to process back-to-back frames - AKA buffering. RFC 2544 measures the number of frames in the largest burst of frames that the DUT can handle without any packet loss.

4 PORTS

4.1 Overview of Ports

Ports can either be set into release or reserve status. By releasing the port, you release ownership of the port, allowing it to be accessed by other users. By reserving the port, the port is retained and can be used in a new “Test Bed.”

Reserving a port will not allow any other users to manage and use this same port.

These options can be enabled by clicking the switch in the Ports section of the Home page.

To create a test bed, the necessary ports must be selected and reserved.

Ports [↗](#)

Ports ID	Status	MAC Address	IP Address	Reserved By	Active Feature	Test Name	Test Status	Reserve/Release
0	UP	00:90:0b:8a:e4:c9	localhost					<input type="checkbox"/>
1	UP	00:90:0b:8a:e4:ca	localhost					<input type="checkbox"/>

[+ Create Testbed](#)

Figure 1: Reserve/Release Ports

4.1.1 Port Reset

The port reset option is located in the ports tab next to Port Reset.

By clicking the icon next to port reset, it will put the ports in resetting mode and refresh all the ports. To use this feature, user must stop all the tests and release all the ports.

You may find this reset option on several screens, such as the administrative screen in the figure below.

Port Reset ↻

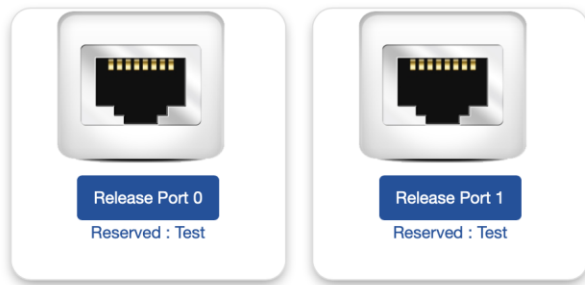


Figure 2: Port Reset

You may also find this Port Reset option right above the Test Bed selection menu, as shown below.

Ports ↻

Ports ID	Status	MAC Address	IP Address	Reserved By	Active Function	Test Name	Test Status	Reserved/Release
0	UP	00:90:0b:8a:e4:c0	localhost	• • •				
1	UP	00:90:0b:8a:e4:ca	localhost	Ports Resetting...				

Figure 3: Test Bed Port Reset

After clicking the reset arrows, the words “Ports Resetting...” will display on the graph while the table momentarily loads and resets the ports. After clicking the reset button, the action cannot be cancelled.

5 TEST BEDS

5.1 Overview of Test Beds

A test bed is a platform used to configure and develop a simulated system. The test bed can be configured to emulate the specific hosts, data streams, and settings needed to accurately reflect the requirements of your system.

5.2 Configuring Test Beds

To create a test bed, select the “Create Testbed” button underneath the Port section. Select “RFC 2544” from the menu and name the test. After naming and selecting the proper menu option, double click to add the new bed to your test environment.

The name of the test can be a maximum of 15 characters.

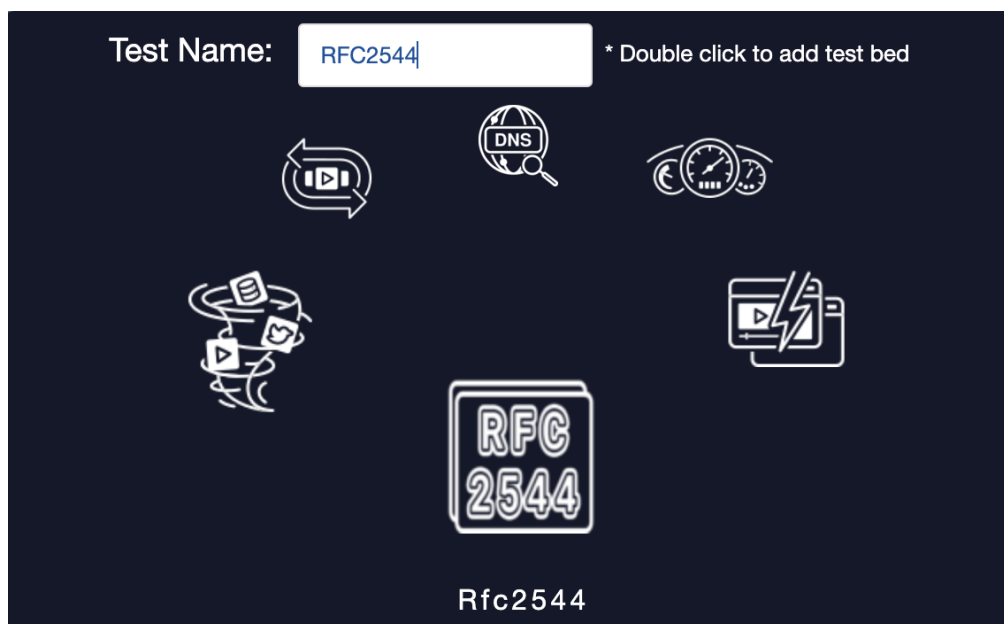


Figure 4: Naming Test Bed

After roughly 60 seconds, the new test bed should appear in the Test Bed section of the home page. Select “Configure” to begin configuring the new test. This operation will redirect you to the five-step configuration menu, starting with Port Reservation.



Figure 5: Configuring Test Bed

6 TEST BED: PORT RESERVATION

6.1 Post Reservation Overview

The Port Reservation menu allows you to add ports to the test bed, set up multi-site configuration, and review the current active ports, their link state, MAC address, IP address, reservation, and feature.

Ports ID	Status	MAC Address	IP Address	Reserve	Feature	Port Reserve
0	UP	00:90:0b:8a:e4:c9	localhost	Test		Add to Test
1	UP	00:90:0b:8a:e4:ca	localhost	Test		Add to Test

Figure 6: Port Reservation Menu

6.2 Adding Ports

To add a Port to a test bed, select the “Add to Test” button on the right side of the Ports Configuration Tab. Selecting this button will automatically add the port to the test and be confirmed with a notification pop-up that the port has been added.

Add all ports that will be needed to develop your test environment.

Ports ID	Status	MAC Address	IP Address	Reserve	Feature	Port Reserve
0	UP	00:90:0b:8a:e4:c9	localhost	Test		Add to Test

Figure 7: Adding Port

6.3 Removing Ports

To remove a Port from the test bed, select the “Remove from Test” button next to the designated Port.

Ports ID	Status	MAC Address	IP Address	Reserve	Feature	Port Reserve
0	UP	00:90:0b:8a:e4:c9	localhost	Test	RFC-2544	Remove from Test

Figure 8: Removing Port

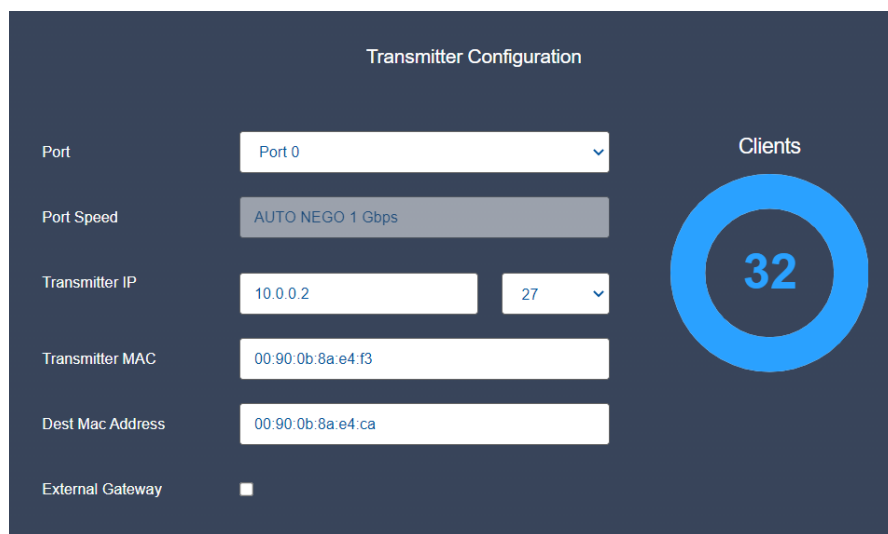
After adding and removing ports, select “Next” to proceed with Traffic configuration.

7 TEST BED: TRAFFIC CONFIGURATION

7.1 Transmitter Configuration

The Transmitter Configuration menu provides options to adjust the following fields:

- ▶ Port
- ▶ Port Speed
- ▶ Transmitter IP
- ▶ Transmitter MAC
- ▶ Dest Mac Address
- ▶ External Gateway
- ▶ Clients



The screenshot displays the 'Transmitter Configuration' interface. On the left, there are several configuration fields: 'Port' is set to 'Port 0'; 'Port Speed' is set to 'AUTO NEGOT 1 Gbps'; 'Transmitter IP' is '10.0.0.2' with a subnet mask of '27'; 'Transmitter MAC' is '00:90:0b:8a:e4:f3'; 'Dest Mac Address' is '00:90:0b:8a:e4:ca'; and 'External Gateway' is currently disabled. On the right side, there is a 'Clients' section featuring a large blue circular gauge with the number '32' in the center, indicating the current number of clients.

Figure 9: Transmitter Configuration

7.1.1 Port

By default, the port value for the transmitter will be set to “Port 0”. To adjust this value, select one of the available ports from the drop-down menu.

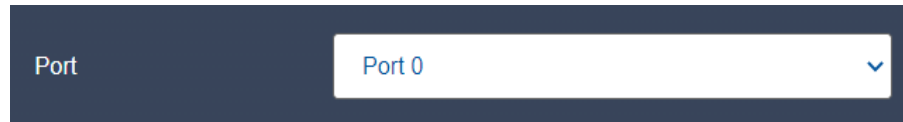
A dark blue rectangular panel with the label "Port" on the left. To its right is a white input field containing the text "Port 0" and a small blue downward-pointing arrow on the right side, indicating a drop-down menu.

Figure 10: Transmitter Port

7.1.2 Port Speed

By default, the Port Speed is set to “AUTO NEGOTIATION X Gbps”. The value of “X” will adjust depending on the type of transceiver in use. For example, a 10 GB transceiver will provide a Port Speed value of “AUTO NEGOTIATION 10 Gbps”. This setting cannot currently be modified.

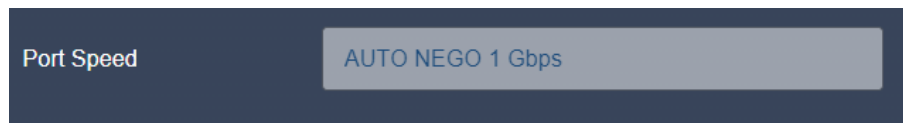
A dark blue rectangular panel with the label "Port Speed" on the left. To its right is a grey rectangular field containing the text "AUTO NEGOTIATION 1 Gbps".

Figure 11: Transmitter Port Speed

7.1.3 Transmitter IP

By default, the IP value will be set to 10.0.0.2 by default.

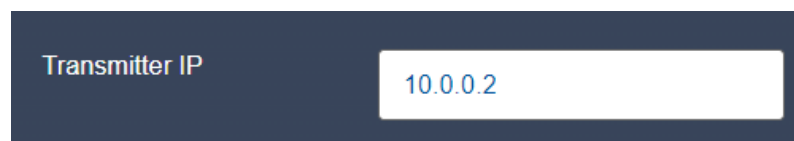
A dark blue rectangular panel with the label "Transmitter IP" on the left. To its right is a white input field containing the text "10.0.0.2".

Figure 12: Transmitter IP

7.1.4 Clients

The number of hosts will adjust according to the CIDR address assigned in the Client IP configuration.

For example, a CIDR value of /27 will correspond to 32 hosts. On the other hand, a CIDR value of /16 will correspond to 65526 hosts.

The following figure depicts the CIDR value of 27:



Figure 13: Clients

To adjust the number of clients, perform one of the following steps:

- ▶ Click on the outer ring of the circle to alter the number of clients.
- ▶ Manually select the center of the circle and enter in a number.

Adjusting the number of clients will result in an allocation of fewer hosts than available on the selected subnet.

7.1.5 Transmitter MAC

By default, the Transmitter MAC address will already be set. To adjust this value, enter the appropriate physical or hardware address.

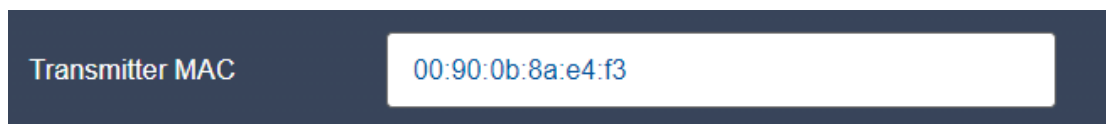
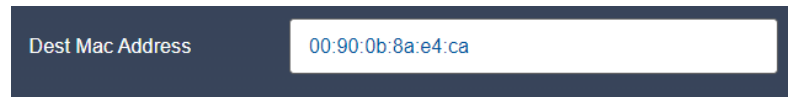


Figure 14: Transmitter MAC

7.1.6 Dest MAC Address

By default, the Destination MAC address will already be set. To adjust this value, enter the appropriate physical or hardware address.

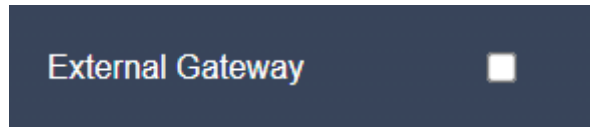


A dark blue rectangular box containing the text "Dest Mac Address" on the left and a white input field on the right containing the hexadecimal value "00:90:0b:8a:e4:ca".

Figure 15: Transmitter Destination MAC

7.1.7 External Gateway

The external gateway will be disabled by default, as shown in the figure below.



A dark blue rectangular box containing the text "External Gateway" on the left and a small white square checkbox on the right, which is currently unchecked.

Figure 16: Transmitter Gateway Disabled

To enable this value, click the check box. Checking this box will display the "Gateway IP" address field and allow you to enter a value into the gateway field.



A dark blue rectangular box containing the text "External Gateway" on the left, a checked checkbox in the middle, and the text "Gateway IP" on the right. To the right of "Gateway IP" is a white input field containing the value "20.0.0.1".

Figure 17: Transmitter Gateway Enabled

7.2 Receiver Configuration

The Receiver Configuration menu provides options to adjust the following fields:

- ▶ Port
- ▶ Port Speed
- ▶ Receiver IP
- ▶ Receiver MAC
- ▶ Dest MAC Address
- ▶ External Gateway

The image shows a 'Receiver Configuration' form with the following fields and values:

Field	Value
Port	Port 1
Port Speed	AUTO NEGO 1 Gbps
Receiver IP	20.0.0.2
Receiver MAC	00:90:0b:8a:e4:ca
Dest Mac Address	00:90:0b:8a:e4:c9
External Gateway	<input type="checkbox"/>

Figure 18: Receiver Configuration

7.2.1 Port

By default, the port value for the receiver will be set to “Port 1”. To adjust this value, select one of the available ports from the drop-down menu.

The image shows a close-up of the 'Port' field, which is a drop-down menu currently displaying 'Port 1'.

Figure 19: Receiver Port

7.2.2 Port Speed

By default, the Port Speed is set to “AUTO NEGO X Gbps”. The value of “X” will adjust depending on the type of transceiver in use. For example, a 10 GB transceiver will provide a Port Speed value of “AUTO NEG 10 Gbps”. This setting cannot currently be modified.

The image shows a close-up of the 'Port Speed' field, which is a text input box containing the value 'AUTO NEGO 1 Gbps'.

Figure 20: Server MAC

7.2.3 Receiver IP

By default, the IP value will be set to 20.0.0.2 by default.

A dark blue rectangular box with a white input field. The label "Receiver IP" is on the left, and the value "20.0.0.2" is entered in the input field.

Figure 21: Receiver IP

7.2.4 Receiver MAC

By default, the Receiver MAC address will already be set. To adjust this value, enter the appropriate physical or hardware address.

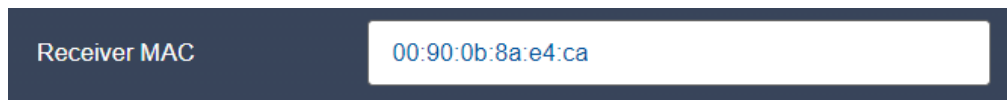
A dark blue rectangular box with a white input field. The label "Receiver MAC" is on the left, and the value "00:90:0b:8a:e4:ca" is entered in the input field.

Figure 22: Receiver MAC

7.2.5 Dest MAC Address

By default, the Dest MAC address will already be set. To adjust this value, enter the appropriate physical or hardware address.

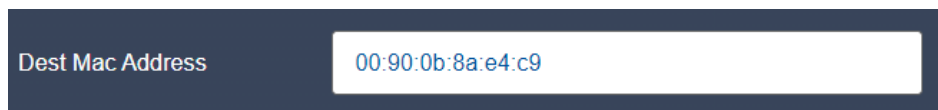
A dark blue rectangular box with a white input field. The label "Dest Mac Address" is on the left, and the value "00:90:0b:8a:e4:c9" is entered in the input field.

Figure 23: Receiver Dest MAC Address

7.2.6 External Gateway

The external gateway will be disabled by default, as shown in the figure below.

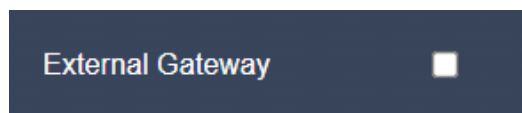
A dark blue rectangular box with the label "External Gateway" on the left and a small white square checkbox on the right.

Figure 24: Receiver Gateway Disabled

To enable this value, click the check box. Checking this box will display the "Gateway IP" address field and allow you to enter a value into the gateway field.



The image shows a dark blue configuration panel. On the left, the text "External Gateway" is followed by a checked checkbox. To the right, the text "Gateway IP" is followed by a white input field containing the IP address "20.0.0.1".

Figure 25: Receiver Gateway Enabled

After configuring the transmitter and receiver, select "Next" to proceed with Test configuration.

8 TEST BED: TEST CONFIGURATION

8.1 Test Configuration Overview

The Test Configuration menu provides checkboxes for the following tests:

- ▶ Throughput Test
- ▶ Latency and Jitter Test
- ▶ Frame Loss Rate Test

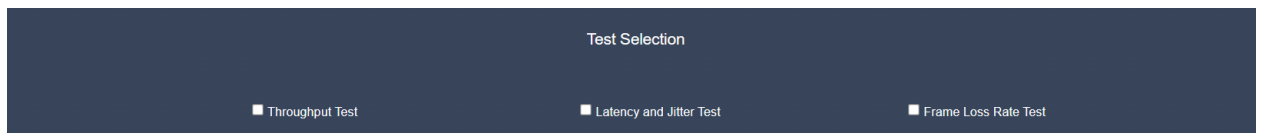


Figure 26: Test Configuration Overview

Once you check a box for the associated test, a menu will become available at the bottom for the test configuration overview for that test. This new available menu will allow you to establish custom packets size, select packet size, adjust number of iterations, and adjust iteration duration.

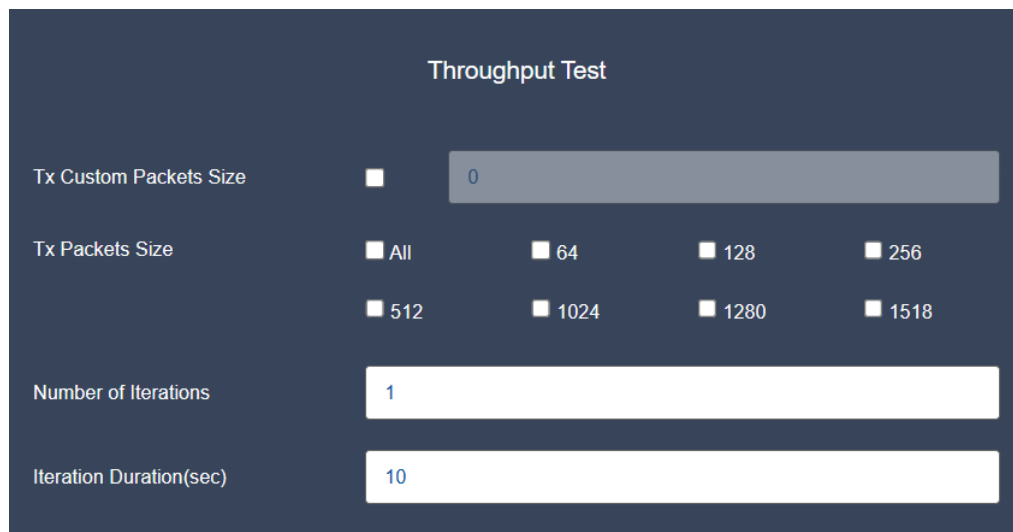


Figure 27: Test Configuration

8.2 Test Configurations

8.2.1 Tx Custom Packets Size

By default, the Tx Custom Packets Size option is disabled. When disabled, data cannot be entered in the custom packets size field. To enable, check the checkbox.



The screenshot shows a dark blue header bar with the text "Tx Custom Packets Size" on the left. To its right is an unchecked checkbox. Further right is a greyed-out text input field containing the number "0".

Figure 28: TX Custom Packets Size Disabled

Once enabled, you can manually enter in a packet size between the sizes of 64 and 9238.

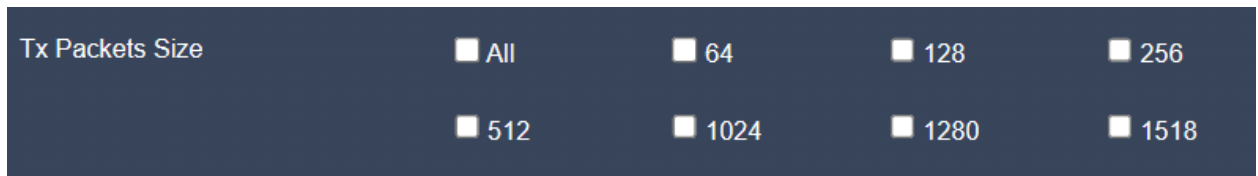


The screenshot shows a dark blue header bar with the text "Tx Custom Packets Size" on the left. To its right is a checked checkbox. Further right is a white text input field containing the number "0".

Figure 29: TX Custom Packets Size Enabled

8.2.2 Tx Packet Size

If a custom packet size isn't entered, a size can be selected from the check box options. More than one packet size can be selected from the menu.



The screenshot shows a dark blue header bar with the text "Tx Packets Size" on the left. To its right are two rows of radio button options. The first row contains "All", "64", "128", and "256". The second row contains "512", "1024", "1280", and "1518".

Figure 30: TX Packets Size

8.2.3 Number of Iterations

To adjust the number of iterations, enter a numeric value in the "Number of Durations" field. This field increases the number of times the test is run.



The screenshot shows a dark blue header bar with the text "Number of Iterations" on the left. To its right is a white text input field containing the number "1".

Figure 31: Number of Iterations

8.2.4 Iteration Duration(sec)

To adjust the Iteration Duration, enter a numeric value in the “Iteration Duration” field. Each value is associated with seconds and will increase how long each iteration lasts.

A dark-themed UI element with a label "Iteration Duration(sec)" on the left and a white input field on the right containing the number "10".

Figure 32: Iteration Duration

8.2.5 Bandwidth Order

To adjust the Bandwidth Order, select either the “Ascending” or “Descending” radio button. “Ascending” will run the test in a step-up fashion, starting at 1% to 100%. “Descending” will run the test in a step-up fashion, starting at 100% to 1%.

A dark-themed configuration panel titled "Frame Loss Rate Test". It contains several settings: "Tx Custom Packets Size" with a value of 0; "Tx Packets Size" with radio buttons for All, 64, 128, 256, 512, 1024, 1280, and 1518 (where 1518 is selected); "Number of Iterations" with a value of 1; "Iteration Duration(sec)" with a value of 10; and "Bandwidth Order" with radio buttons for Ascending (selected) and Descending.

Figure 33: Bandwidth Order

After selecting the test and configuring each applicable test, select “Next” to proceed with Protocol Segment.



For Throughput Test and Frame Loss Test Iteration Durations should not be less than 10 seconds.

For the Latency and Jitter Test, the Number of Iterations and Iteration Duration must be set to at least 10.

9 TEST BED: PROTOCOL SEGMENT

9.1 Protocol Segment Overview

The Protocol Segment overview menu provides a detailed overview of the protocol streams associated with your test and allows you add, configure, or delete streams.

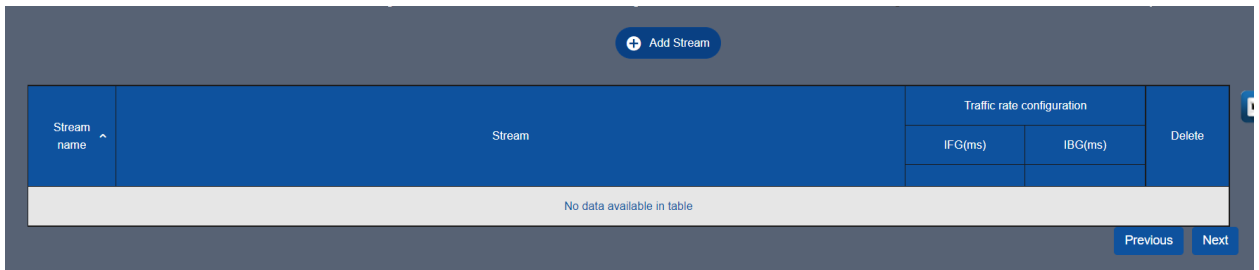


Figure 34: Protocol Stream Menu

By clicking the “Add Stream” button at the top of the menu, you will be able to add a stream to the test bed.

9.2 Adding Streams

Select the “Add Stream” button at the top of the menu, as demonstrated in Figure 32. Enter a name for the stream and select the desired stream from the drop-down menu.

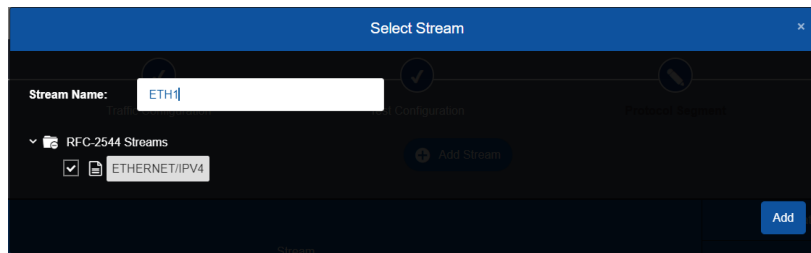


Figure 35: Traffic Configuration

9.3 Configuring Streams

After a stream has been added, adjust the traffic rate configuration for each stream, as needed.

Stream name	Stream	Traffic rate configuration		Delete
		IFG(ms)	IBG(ms)	
ETH1	ETHERNET IP	0	0	

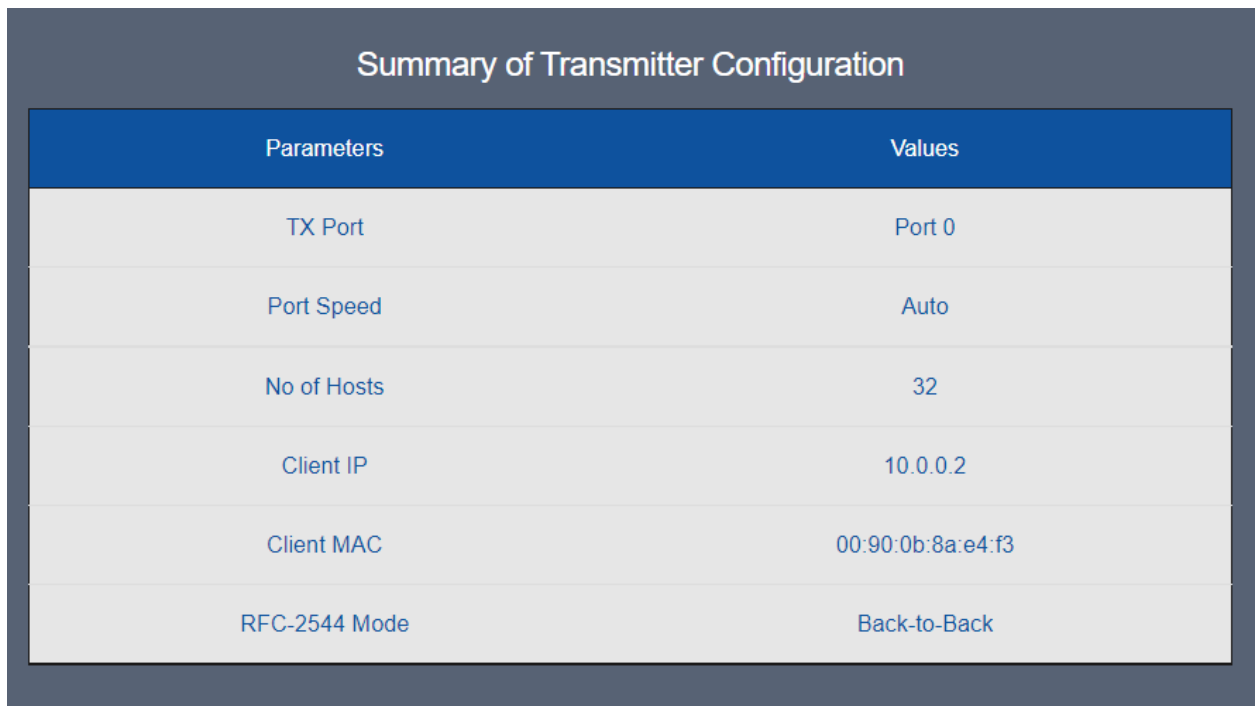
Previous Next

Figure 36: Stream Traffic Rate Configuration

10 TEST BED: SUMMARY

10.1 Summary of Transmitter Configuration

The Summary of Transmitter Configuration provides an overview of the configuration settings selected for the transmitter.



The screenshot shows a table titled "Summary of Transmitter Configuration" with two columns: "Parameters" and "Values". The table lists the following configuration settings:

Parameters	Values
TX Port	Port 0
Port Speed	Auto
No of Hosts	32
Client IP	10.0.0.2
Client MAC	00:90:0b:8a:e4:f3
RFC-2544 Mode	Back-to-Back

Figure 37: Summary of Transmitter Configuration

10.2 Summary of Receiver Configuration

The Summary of Receiver Configuration provides an overview of the configuration settings selected for the receiver.

Summary of Receiver Configuration	
Parameters	Values
RX Port	Port 1
Port Speed	Auto
Server IP	20.0.0.2
Server MAC	00:90:0b:8a:e4:ca
RFC-2544 Mode	Back-to-Back

Figure 38: Summary of Receiver Configuration

After reviewing the summaries, select "Start Test" button to begin testing.

11 STATISTICS

The Netropy Traffic Generation RFC 2544 platform provides Aggregate Statistics, Test Statistics, and Offline Analyzer results. All results can be viewed in the Statistics window of the GUI.

11.1 Aggregate Statistics

The Aggregate Statistics tab provides detailed results for the test across all applications. This tab provides the following information:

- ▶ Statistics Table
- ▶ Client Statistics
- ▶ Server Statistics
- ▶ Throughput Graph (Gbps)
- ▶ Packets/Second Graph (Mpps)
- ▶ Latency Graph (ms)

The aggregate statistics table provides a tabular view of the data collected during the test.

Port^	TxPkts	RxPkts	Tx(Gbps)	Rx(Gbps)	Latency(ms)	TxTotalPkts	RxTotalPkts	TxTotal(Gb)	RxTotal(Gb)	AvgTxPkts	AvgRxPkts	AvgTx(Gbps)	AvgRx(Gbp
P0	119275	0	1.00	0.00	0	9080708	1192702	76.13	10.00	3090	411	0.03	0.00
P1	0	119275	0.00	1.00	0.252	1192750	9196880	10.00	77.11	360	3098	0.00	0.03

Figure 39: Aggregate Statistics Table

To adjust the fields shown in the table, select the blue hamburger menu icon. All fields are selected by default and unchecking a field will remove it from the graph's display.

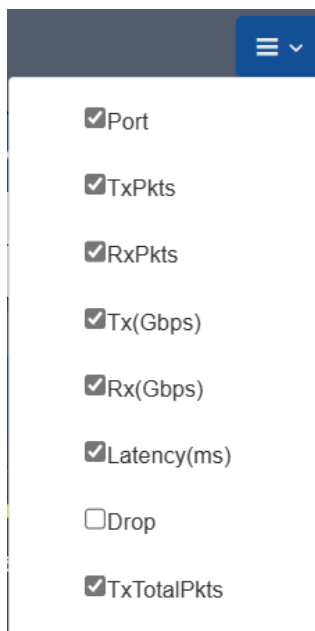


Figure 40: Statistics Filter

These statistics are further defined in Section 11.4.

The following charts depict the Server Statistics, including Throughput and Million Packet Per Second (MPPS).



Figure 41: Client Statistics

The following charts depict the Server Statistics, including Throughput and MPPS.



Figure 42: Server Statistics

Following these charts, there are numerous graphs that provide additional information.

Each of these graphs will provide information for each of the ports associated with the test. The graph settings will allow you to select either of the ports for transmission or received packets, as shown in the Throughput Graphs below.

There are also options to view the graph in either ascending or descending order, which displays the values starting at 1% (Ascending) or starting at 100% (Descending).

Refer to the following graph for the Ascending view:

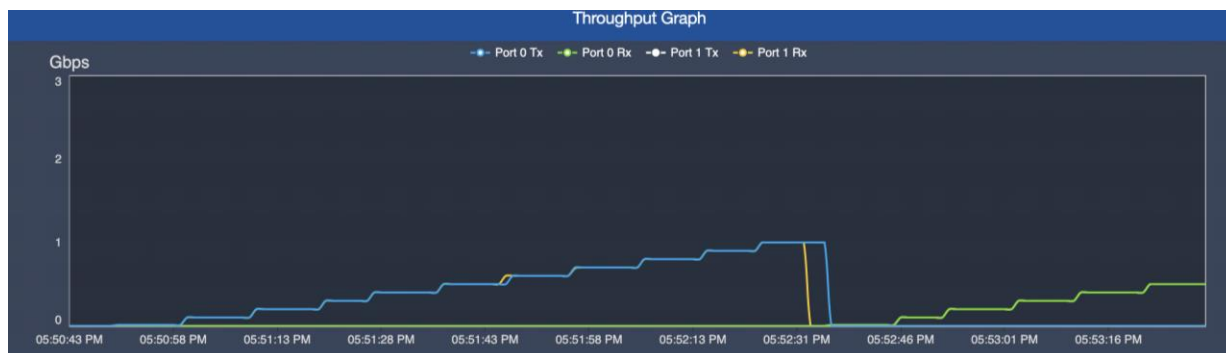


Figure 43: Throughput Graph (Ascending)

Refer to the following graph for the Descending view:

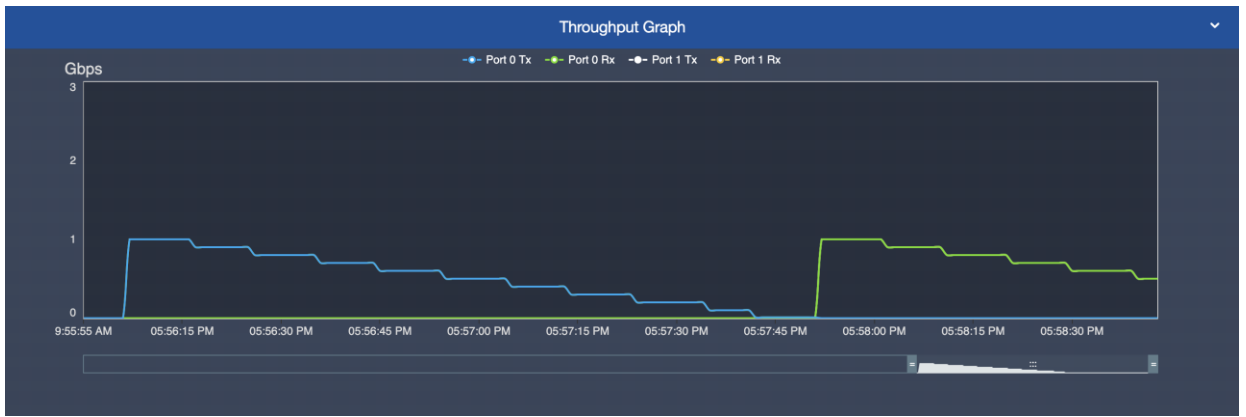


Figure 44: Throughput Graph (Descending)

11.2 Test Statistics

The Test Statistics tab provides detailed results for each of the selected tests. This tab provides the following information:

► Throughput Test Graph

This section provides two graphs. One for data from East to West and another for data from West to East.



Figure 45: Throughput Test Graph

► Latency and Jitter Test Graph

This section provides four graphs. One for data from East to West and another for data from West to East for both tests – Latency and Jitter.

These graphs also are color-coded to show Min Latency, Max Latency, and Avg Latency.

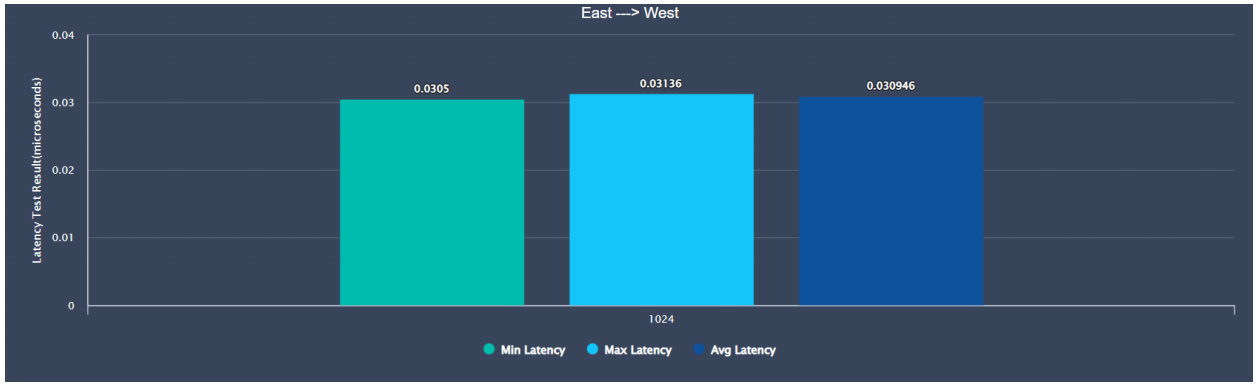


Figure 46: Latency Test Graph

► Frame Loss Rate Test Graph

This section provides two graphs. One for data from East to West and another for data from West to East.

These graphs also are color-coded to show Bandwidth at the following percentages: 100%, 90%, 80%, 70%, 60%, 50%, 40%, 30%, 20%, 10% and 1%.

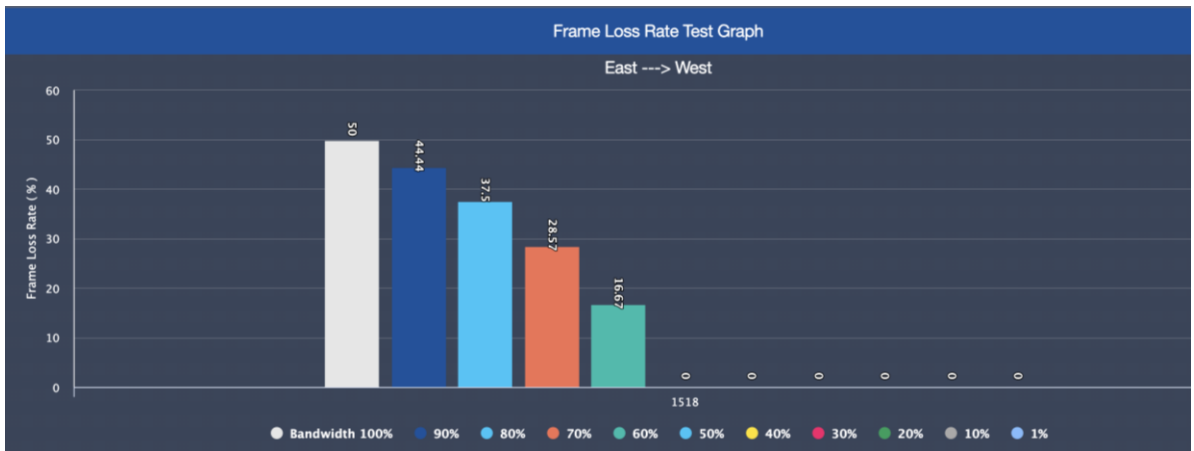


Figure 47: Frame Loss Rate Test Graph

11.3 Offline Analyzer

The Offline Analyzer tab provides the following graphs:

- Packets/Second
- Throughput
- Latency

To download, select the download icon on the right of the graph and hover over “Download as...” to present the available download options.

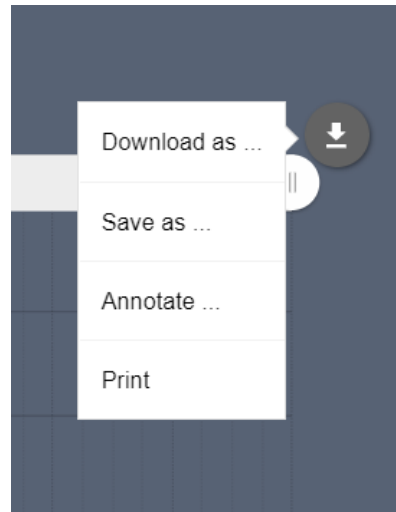


Figure 48: Downloading Graphs

Each of these graphs can be downloaded individually in either PDF, JPG, SVG, or PNG format. To select a file format, click your desired format from the menu. The selected file will be downloaded directly to your computer’s default file location for downloads.

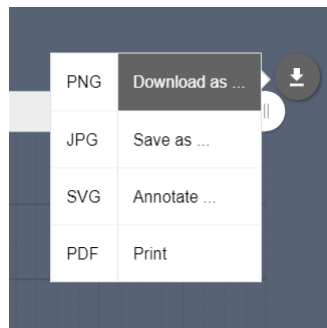


Figure 49: Download File Options

In addition, each graph can be saved as a CSV, JSON, or XSLX file. To select one of these options, hover over the “Save as...” option and select the desired file format.



Figure 50: Save As File Options

To print the graph, select the “Print” option from the menu shown in the figure above. This will open your browser’s printing menu and allow you to select your default printer and settings.

These graphs also may be annotated using the built-in illustration feature. These annotated graphs can also be downloaded in the same formats. To annotate a graph, select the “Annotate...” option from the menu.

Selecting this menu option will turn the graph white and allow you to annotate the graph. Users can add shapes and text directly to the graph. In addition, users are allowed to change the color and mode of the marker and text.

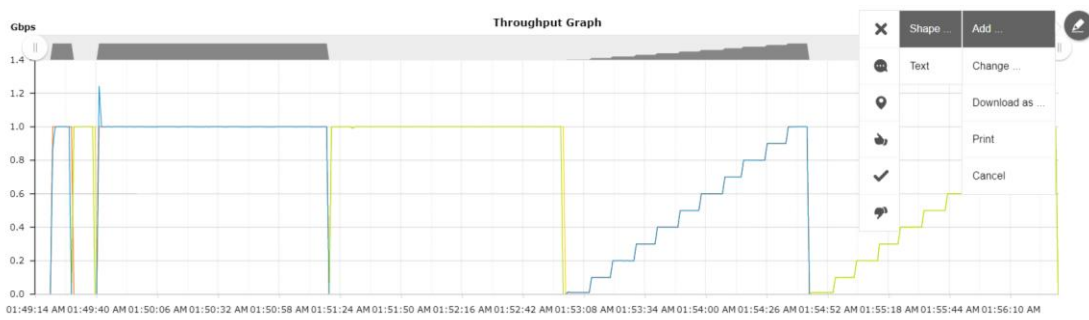


Figure 51: Annotate Graph

To change the annotated graph, hover on the edit pen on the top right corner of the graph and select “Change”.

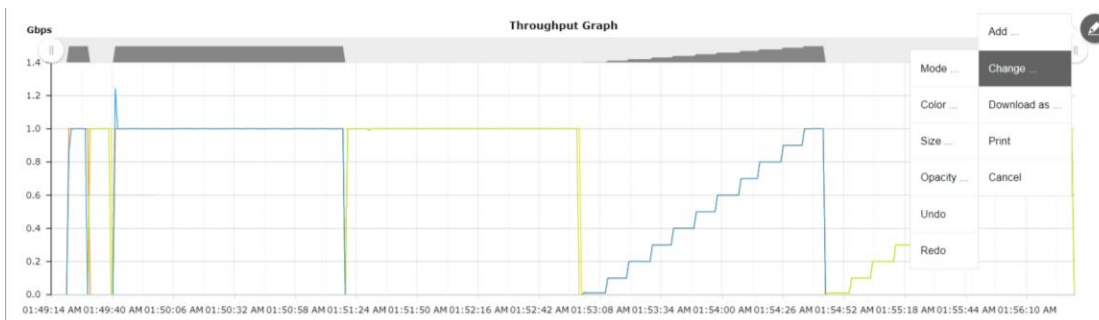


Figure 52: Change Graph

The annotated graph can be printed or downloaded in either PNG, JPG, SVG, or PDF format.

11.4 Definitions: Statistics

The following table includes the definition of various statistics displayed in the graphs and tables provided by RFC 2544:

Statistic	Description
Port	The Port Number for which statistics are shown.
TxPkts	The number of packets transmitted on the port in the last 1 second interval.
RXPkts	The number of packets received on the port in the last 1 second interval.
TX (Gbps)	The rate of packets transmitted (in Gigabits per second) on the port in the last 1 second interval.
RX (Gbps)	The rate of packets received (in Gigabits per second) on the port in the last 1 second interval.
Latency(ms)	The time (in milliseconds) taken by the packet to be received on the Destination port from the time it was transmitted on the Source port. This is calculated as an average for all the packets received in the last 1 sec interval.
Drop	The total number of packets dropped on the Port from the time test was started. The drop counter gets updated only when the test stops.
TxTotalPkts	The total number of packets transmitted on the port from the time test was started.
RxTotalPkts	The total number of packets received on the port from the time test was started.
TxTotal(Gb)	The total number of gigabits transmitted on the port from the time test was started.
RxTotal(Gb)	The total number of gigabits received on the port from the time test was started.
AvgTxPkts	The total number of gigabits transmitted on the port from the time test was started.
AvgRxPkts	The total number of gigabits received on the port from the time test was started.

AvgTx(Gbps)	The average rate of packets transmitted (in Gigabits per second) on the port per second from the time test was started.
AvgRx(Gbps)	The average rate of packets received (in Gigabits per second) on the port per second from the time test was started

12 TEST SETTINGS

The test provides options to capture pcaps, pause, play, stop, and clear statistics. The following sections will provide additional details on these configurations.

12.1 Play/Pause/Stop

To adjust the play, pause, and stop settings for a test, select the power button on the right side of the screen.



Figure 53: Play/Pause/Stop Settings

Selecting this button will present a menu to select the pause, play, and stop buttons. When the test is stopped, the test bed will initiate the generation of a report. This report will be available within the Logs tab. If a test is paused, the user will be notified and provided the option to replay in the same menu.

If a test is played, the user will be provided the option to either pause or stop the test.

12.2 Clear Statistics

To clear the current statistics, hover over the broom icon on the left side of the screen and select "Clear Statistics". This action will clear all statistics shown in the available graphs but will not alter the contents of the Log files.



Figure 54: Clear Statistics

12.3 Start Packet Capture

To start a network packet capture of the traffic that occurs during your test, hover over the camera icon on the left side of the screen to present a green button labeled “Start Capture”. Click this button to begin a network packet capture.



Figure 55: Network Capture

13 LOGS

13.1 Logs Overview

Logs may be collected from tests to use for analysis and review by users. The system will collect and maintain these logs for future use. These files can be found within the Logs tab of the Statistics menu.

The size of these log files will vary based on the amount of data collected and the number of packets selected within the capture. All capture files will be provided in .pcap form to ensure they are compatible with Wireshark and similar software programs.

13.2 Managing Logs

The Logs tab of the Statistics window presents a list of available reports. These reports can be downloaded or deleted.

To download a report, select the download icon on the specified file. This will download a zip folder to the default download location on your device. To delete a file from the logs, select the trash can icon on the specified file.

To delete all logs, select the “Delete All” button in the top right corner.

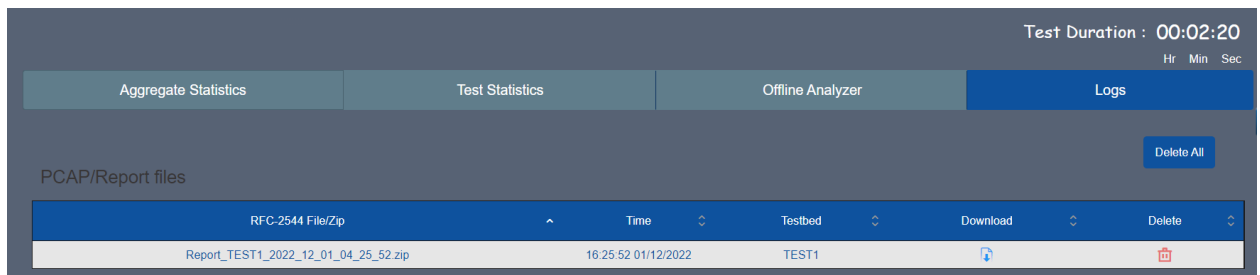


Figure 56: Logs Tab



If you select the delete icon or button, you will not be presented with a confirmation window. Unless previously downloaded, you cannot retrieve deleted reports.

13.3 Log Files

After a report has been downloaded, right click the zip folder, and select “Extract All” to extract the file’s content to another location. The extracted folder may include some the following files:

- ▶ Offline Analyzer Latency (CSV)

This file includes latency data collected from the test.

- ▶ Offline Analyzer PPS (CSV)

This file includes packets per second of data collected from the test.

- ▶ Offline Analyzer Throughput (CSV)

This file includes throughput data collected from the test.

- ▶ Configuration (XML)

This file includes the test bed configuration, which can be imported into the test later.

- ▶ Test Report Document (PDF)

The file includes a PDF summary of the test configuration and relevant statistics recorded from the test.

14 ADMINISTRATION

The Netropy Traffic Generation RFC 2544 can be administered through the Administration portal accessible via browser. The administrator must log in using their administrative credentials.

14.1 User Settings

The User tab presents options to add, edit, and delete users. By default, there will only be a single user account, the administrator. To create additional accounts to manage and configure test beds, the administrator must add new users.

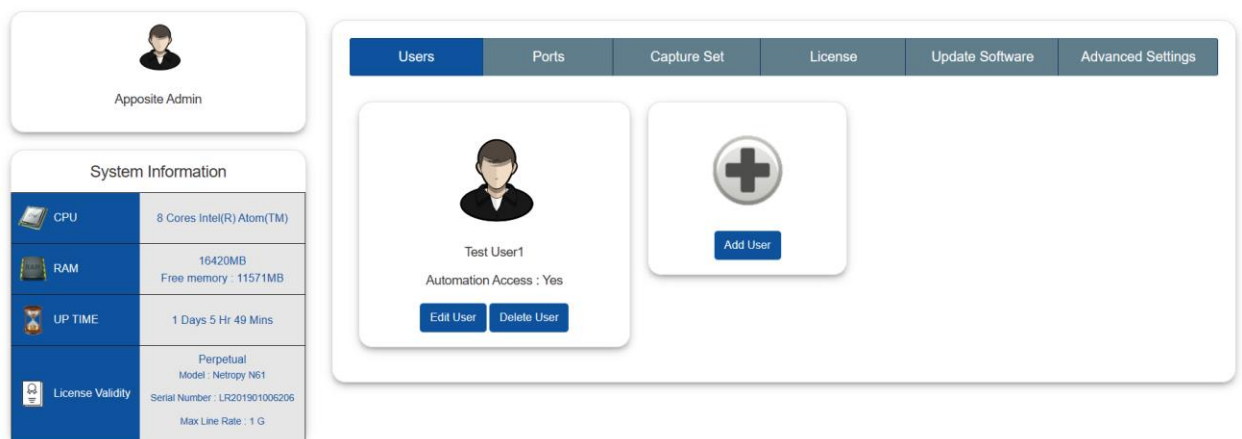


Figure 57: User Tab

When adding a new user, the following information is required:

- ▶ First Name
- ▶ Last Name
- ▶ User Name
- ▶ Email
- ▶ Password
- ▶ Automation Access

- ▶ The account will be created once the “Create User” button is selected. This user will then be able to access the configuration portal using their new credentials. Only the administrator will have access to these permissions. Other users will be able to make configuration changes but will not have privileges to access and manage other accounts.

▶ **Figure 58: New User**

14.2 Port Settings

The Port tab displays the status of ports and allows the administrator to manually release ports as needed. This will override any port releases and reservations made by other user accounts.

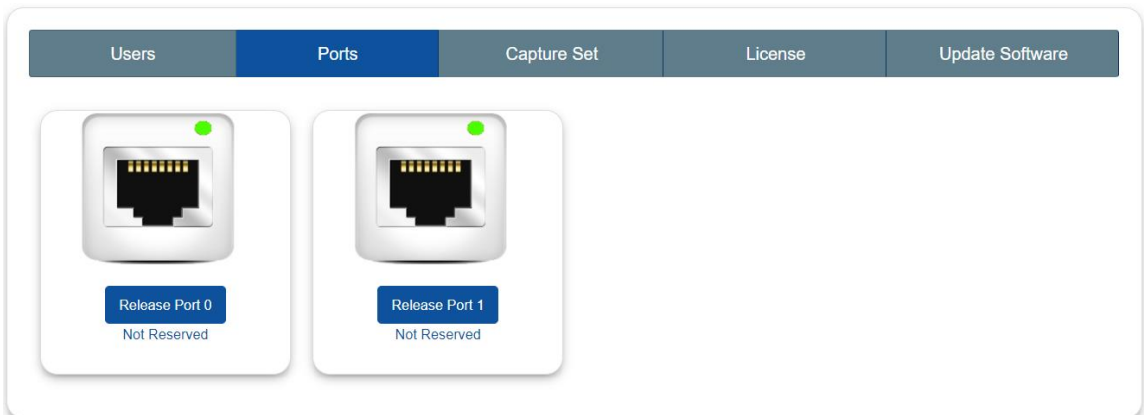


Figure 59: Port Tab

To release a port, click on the associated “Release Port X” button. As demonstrated in the figure below, this button will open a pop-up that displays the IP Address, status, speed, MAC address, and details on whether the port is reserved. By clicking “Release” the port will be released.

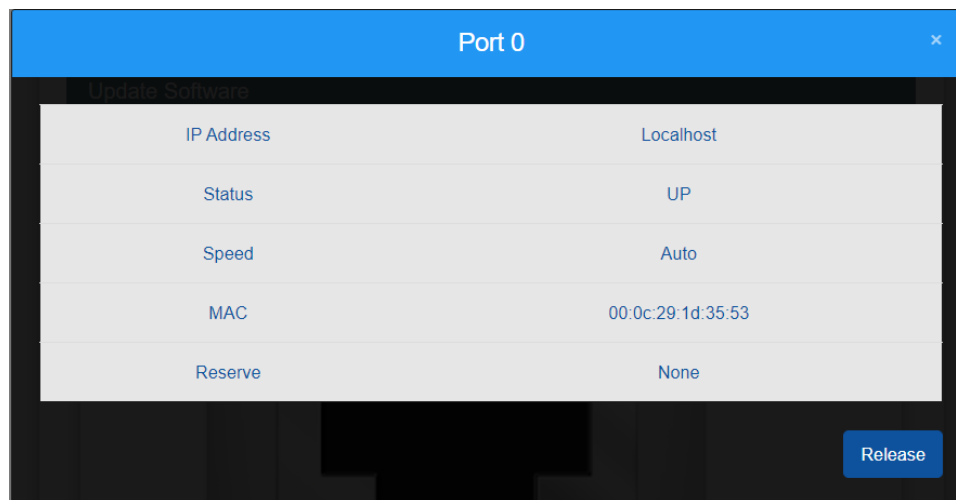


Figure 60: Release Port Settings

14.3 Capture Settings

RFC 2544 can be configured to capture a specific number of packets during a session. By default, the number of packets to capture will be set to 100 packets. This setting can easily be altered by clicking the drop-down menu, as shown in the figure below. Options in this menu will range from 100 packets to 1,000,000 packets.

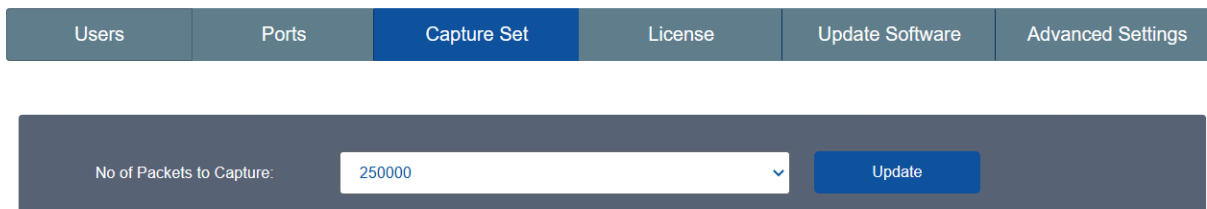


Figure 61: Capture Settings

Click “Update” to initiate these changes and ensure all future packet sessions will capture the specified number of packets.

14.4 License Settings

The License tab will display the license, license type, license validity, and the number of licensed ports. To obtain additional information on how to renew a license, visit <https://www.apposite-tech.com/renewals/> to submit a renewal request form.

To add a license key, click the “Browse” button to search for files on your device. After selecting the applicable file, click “Open” in file explorer. Then, proceed by selecting “Upload” to upload the

license key file into the system.

License	Valid
License Type	TrafficEngine, AppStorm, AppPlayback RFC-2544, SessionStrike, DNS Storm
License Validity	6 Aug, 2121
Number of Licensed Ports	2

License File

Figure 62: License Tab

14.5 Update Software Settings

The Update Settings tab allows the selection of a BIN file to update the system software. To update the BIN file, select the plus button icon, and select the appropriate file on your PC. After selecting the file, the system will request a system reboot. Select “Yes” to allow the system to apply all necessary patches and updates.

Upload Bin file

Figure 63: Update Software Tab

14.6 Advanced Settings

The Advanced Settings tab allows management of time zone, signature, binary search, DNS Queries File, Authentication, NAS IP, and Secret Key.

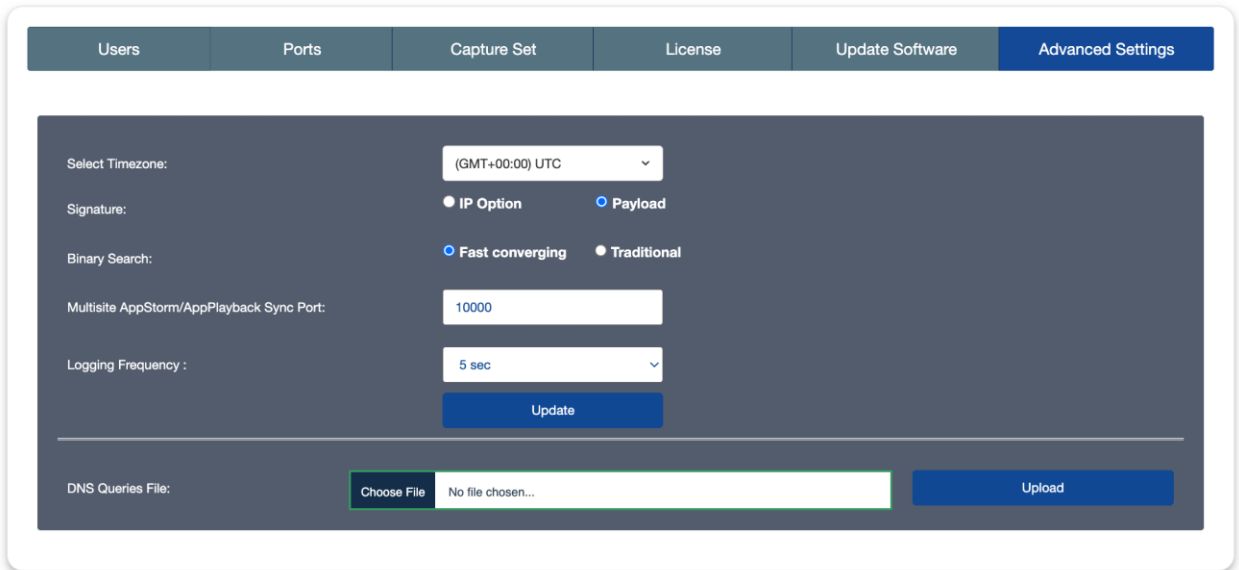


Figure 64: Advanced Settings

14.7 Time Zone

Users can select the time zone of their location. To select the time zone, click the down arrow next to the default time by the “Select Timezone” value.

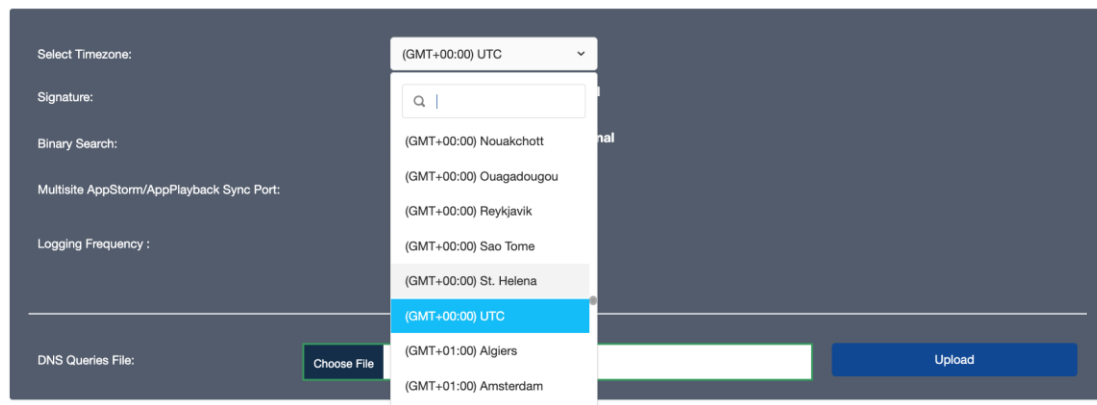


Figure 65: Time Zone

14.8 Signature

The selection determines where the control information used by NTG gets stored in the packets being transmitted.

1. **IP Options:** In this case, the control information is stored in the IP options field in the IP

header.

2. **Payload:** In this case, the control information is stored in the IP Payload.

To select one of the two options, select the applicable radio button. Then, click “Update” to complete the change.



The image shows a dark grey rectangular panel. On the left side, the text "Signature:" is displayed. To the right of this text are two radio button options. The first option is "IP Option" and is selected, indicated by a solid white dot inside the radio button. The second option is "Payload" and is not selected, indicated by an empty white circle inside the radio button.

Figure 66: Signature

14.9 DNS Queries File

This is the file which consists of the lists of domain names which are used by the DNS Storm feature when sending DNS queries. DNS Storm feature cycles through this list of domain names.

Select “Browse” to choose the appropriate DNS Queries File. Then, click “Update” to complete the change after the file has been selected.



The image shows a dark grey rectangular panel. On the left side, the text "DNS Queries File :" is displayed. To the right of this text is a blue rectangular button with the word "Browse" written in white text.

Figure 67: DNS Queries File

15 COMMAND LINE INTERFACE

The Netropy command line interface (CLI) can be accessed via the CONSOLE interface or through a Telnet or SSH connection.

The following are the only features available through the CLI:

- ▶ ARP and PING commands
- ▶ Reinitialize the unit to factory settings
- ▶ Management functions

To access the CLI, log into the device at the prompt as “admin” or other configured username.

15.1 CLI Help

The CLI includes several levels of help. The “help” command by itself displays a list of commands. “help” with a command name displays the syntax and options for the command.

When entering commands, the <Tab> key can be used to complete a partially entered command name. If there are multiple possible completions, pressing the <Tab> key again will display a list of options.

15.2 CLI Top Level Commands

Command	Syntax and Description
arp	<code>arp show</code> Displays a table of IP addresses and associated MAC addresses for the MGMT interface.
clock	<code>clock show</code> Displays the current system time and date.
help	<code>{help ?} [<command>]</code> Displays a list of available commands or syntax of a specified command. A question mark after any command also displays the syntax for that command.

init	<pre>init config</pre> <p>Returns the configuration to factory default settings. Takes effect upon reboot unless the configuration is saved prior to reboot.</p>
logout	<pre>logout</pre> <p>Logout from the command line interface.</p>
mgmt	<pre>mgmt show</pre> <p>Displays the IP address and other management information.</p> <pre>mgmt show ntp associations</pre> <p>Displays the synchronization state with the configured NTP servers.</p> <pre>mgmt set addr {dhcp addr <addr> netmask <mask>}</pre> <p>Sets the IPv4 address and netmask of the MGMT interface either manually or using DHCP. If DHCP is enabled, DHCP sets the default gateway.</p> <pre>mgmt set domain <domain></pre> <p>Sets the network domain name of the device.</p> <pre>mgmt set gw <addr></pre> <p>Sets a default gateway for the MGMT interface.</p> <pre>mgmt set hostname <name></pre> <p>Sets the hostname of the device.</p> <pre>mgmt set nameserver <addr> [<addr2> [<addr3>]]</pre> <p>Sets up to three DNS servers for the device. This command overrides any nameservers set through DHCP and any DNS servers previously configured.</p> <pre>mgmt set ntp server <server> [<server2> [<server3>]]</pre> <p>Sets up to three network time protocol servers for the device. This command overrides any NTP servers set through DHCP and any NTP servers previously configured.</p>
mgmt	<pre>mgmt clear nameserver</pre> <p>Clears all manually configured DNS servers. Does not change any DNS servers set through DHCP.</p> <pre>mgmt clear ntp server</pre> <p>Clears all manually configured NTP servers. Does not change any NTP servers set through DHCP.</p>
ping	<pre>ping <ip-address> [<size>]</pre> <p>Pings from the device to the IP address with the specified sized packets using the MGMT interface. Use CTRL-C to stop.</p>
reboot	<pre>reboot</pre> <p>Reboots the device. Returns user to the login prompt after reboot.</p>
Serial number	<pre>serialnumber</pre> <p>Displays the serial number of the unit.</p>

upgrade	<pre>upgrade <upgrade-image-url></pre> <p>Upgrades the Netropy firmware. FTP, HTTP, and TFTP services are supported. Ex: upgrade ftp://server/netropy-image</p>
Version	<pre>version</pre> <p>Displays the operating firmware version.</p>

15.3 RADIUS Management Commands

Command	Syntax and Description
show	<pre>mgmt show radius</pre> <p>Displays the current RADIUS configuration.</p>
set	<pre>mgmt set radius server <server></pre> <p>Identifies the RADIUS server by IP address or host name. Communication to RADIUS server occurs over the default port 1812. Ex.: mgmt set radius server radiusserver.example.com</p> <pre>mgmt set radius secret <secret></pre> <p>Set the shared secret that the RADIUS server uses to authorize the client. Ex.: mgmt set radius secret secret_key</p> <pre>mgmt set radius { on off }</pre> <p>Turns RADIUS authentication on or off.</p>
clear	<pre>mgmt clear radius</pre> <p>Turns off RADIUS authentication and clears the RADIUS configuration.</p>

15.4 LDAP Management Commands

Command	Syntax and Description
show	<pre>mgmt show ldap</pre> <p>Displays the current RADIUS configuration.</p>

<p>set</p>	<pre> mgmt set ldap server <server> [port <#>] Identifies the LDAP server by IP address or host name. Optionally specifies a non-standard port to connect to. The default port is 389. Ex.: mgmt set ldap server ldapserver.example.com mgmt set ldap basedn <search-base-DN> Identifies the Distinguished Name of the search based in the remote LDAP database. If there are embedded spaces in the base DN string, the string must be enclosed in quotation marks. Ex.: mgmt set ldap basedn dc=example,dc=com mgmt set ldap filter attribute <string> [<LDAP-search-string>] Specifies the attribute that contains the username and optionally an additional LDAP search string. The LDAP search string must be compatible with the formal definition found in RFC 4515. If there are embedded spaces in the search string, the string must be enclosed in quotation marks. Ex.: mgmt set ldap filter attribute uid & (&(gidNumber=20)(class=Expert)) The resulting search string will be (&(uid=user) (&(gidNumber=20) (class=Expert))) where "user" is replaced by the login name. mgmt set ldap security {disable enable} Enable or disable Transport Level Security. TLS is enabled by default. mgmt set ldap bind dn <bind-DN> [password <password>] Specifies a Distinguished Name and password with which to bind to the LDAP server before performing a search operation. If not configured, an anonymous bind will be used. Ex.: mgmt set ldap bind dn cn=user, dc=example,dc=com mgmt set ldap { on off } Turns LDAP authentication on or off. </pre>
<p>clear</p>	<pre> mgmt clear ldap Turns off LDAP authentication and clears the LDAP configuration. </pre>

16 SECURITY

16.1 Users and Passwords

Initially, the RFC 2544 system has a single user configured with the following credentials:

- ▶ Username: admin
- ▶ Password: admin

Refer to Section 14 for additional information on proper management and addition of user accounts through the GUI interface.

17 APPOSITE SUPPORT

17.1 Registration

For access to the Netropy Traffic Generation support site with firmware upgrades, documentation, and other support materials, register your unit at: <http://www.apposite-tech.com/register.html>.

Registered users will receive an email notification whenever new firmware versions are released.

17.2 Customer Support

If you experience any problems with the Netropy Traffic Generation hardware, consult the *Hardware Guide* for your intended model. If you have any questions about the firmware that have not been answered in this *User's Guide*, please check the Apposite Technologies website at <http://www.apposite-tech.com> for updated firmware and supporting documentation. If the answer to your inquiry is not answered on the website, please contact Apposite Support.

All units with an active product license may receive support and maintenance for the term of the license. This support includes hardware warranty, firmware updates, and customer support. The license expiration date for limited-term licenses is shown in the Administrative portal of the Netropy Traffic Generation system on the info page.

License renewals are available from Apposite or the reseller of your unit.

If you believe the firmware is not functioning properly, please upgrade to the latest firmware release. If the problem persists, please contact Apposite Support at:

- ▶ support@apposite-tech.com
- ▶ 1.310.477.9955 ext. 2

When contacting Apposite Support, please include the following information with your request:

- ▶ Model number
- ▶ Serial number
- ▶ Your name
- ▶ Your e-mail address and phone number

- ▶ Installed firmware version
- ▶ A detailed description of the problem



Do not attempt to fix any hardware problem yourself. RFC 2544 hardware devices do not contain any user-serviceable parts. Opening the chassis voids the warranty.

APPENDIX A:

APPOSITE END USER LICENSE AGREEMENT

THIS END USER LICENSE AGREEMENT (“AGREEMENT”) IS A LEGAL AGREEMENT BETWEEN YOU AND APPOSITE TECHNOLOGIES LLC (“APPOSITE”). BY DOWNLOADING, INSTALLING, COPYING, ACCESSING, OR USING THIS SOFTWARE, YOU AGREE TO THE TERMS OF THIS AGREEMENT. IF YOU ARE ACCEPTING THESE TERMS ON BEHALF OF ANOTHER PERSON OR COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT AND WARRANT THAT YOU HAVE FULL AUTHORITY TO BIND THAT PERSON, COMPANY, OR LEGAL ENTITY TO THESE TERMS. IF YOU DO NOT AGREE TO THESE TERMS, ARE NOT AT LEAST 18 YEARS OF AGE, OR DO NOT HAVE AUTHORITY TO ENTER THIS AGREEMENT, DO NOT DOWNLOAD, INSTALL, COPY, ACCESS OR USE THIS SOFTWARE, AND PROMPTLY RETURN THIS SOFTWARE AND PROOF OF ENTITLEMENT TO THE PARTY FROM WHOM YOU ACQUIRED THEM.

1. DEFINITIONS.

- a. "Documentation" means published user manuals and other explanatory materials provided by Apposite relating to the Software or the Hardware.
- b. "Hardware" means the Apposite-branded hardware product on which the Software is designed to run.
- c. "Software" means the computer software (regardless of format or media in which distributed) designed to run on the Hardware.
- d. "Modifications" means any applicable upgrades, modified versions, updates, bug fixes, patches, or other modifications to the Software made generally available by Apposite to its customers.
- e. "Product" means the Apposite-branded product comprised of the Hardware, the Software, and the Documentation.
- f. "Legacy Product" means any Product purchased prior to August 1, 2017.
- g. "License Period" means for any Product that is not a Legacy Product, the license period identified on the relevant order form or receipt upon your purchase of the Product or the Software, including any purchased extension thereto.
- h. "Warranty Period" means (a) for any Legacy Product, the period during which you maintain a continuous, active subscription to Apposite maintenance services, or (b) for any Product that is not a Legacy Product, the License Period, unless such Product has a perpetual license, in which case the Warranty Period shall be five (5) years from the date of purchase of the Product from Apposite unless extended by purchase of maintenance services.

2. LICENSE GRANT. Conditioned upon compliance with the terms and conditions of this Agreement, Apposite hereby grants you the following licenses (collectively, the "License"):

- a. With respect to any Product that is not a Legacy Product, for the relevant License Period, a nonexclusive, nonsublicensable, nontransferable license to use the Software and Modifications solely as embedded in the Hardware, and to use the Documentation solely in conjunction with the Software, Modifications, and Hardware; and
- b. With respect to any Legacy Product, a perpetual, nonexclusive, nonsublicensable, nontransferable license to use the Software solely as embedded in the Hardware, and to use the Documentation solely in conjunction with such Software and Hardware, and to use any Modifications released by Apposite and installed on the Hardware during the Warranty Period.

This license is not a sale. The Software may contain open source or third-party software, subject to separate license terms. Acknowledgements, licensing terms and disclaimers for such materials are contained in the Documentation, and your use of such material is governed by their respective terms and not by the License.

3. **OWNERSHIP.** Apposite and its licensors retain ownership of all intellectual property rights in and to the Software and Documentation, including any copies, improvements, enhancements, derivative works, and modifications thereof. The Software and Documentation are protected by United States and international copyright and other intellectual property laws and international trade provisions. Your rights to use the Software and Documentation are limited to those expressly granted by this Agreement. No other rights with respect to the Software or any related intellectual property rights are granted or implied.

4. **RESTRICTIONS.** Except as otherwise expressly provided under this Agreement, you shall not directly or authorize any third party to:
 - (i) copy the Software, except as necessary for archival or backup purposes only;
 - (ii) transfer, assign, sublicense, rent, lease, lend, or otherwise transfer your license rights to any other person or entity;
 - (iii) install or use the Software on any computing device other than the Hardware;
 - (iv) modify or adapt the Software or Documentation or create derivative works based upon the Software or Documentation;
 - (v) reverse engineer, disassemble, decompile, decrypt, or otherwise attempt to derive the source code of the Software, except to the extent otherwise expressly permitted under applicable law notwithstanding this restriction; or
 - (vi) remove, alter, cover, or obfuscate any of the trademarks, trade names, logos, patent or copyright notices or markings, or add any other notices or markings to or on the Software, Documentation, or Hardware without the express written authorization of Apposite.

5. **SUPPORT.** Apposite shall have no obligation to support the Software except as provided in Apposite's Customer Support Terms and Conditions, which is incorporated by reference into this Agreement.

6. **LIMITED WARRANTY.** Apposite warrants that, for the duration of the Warranty Period, the Hardware will be free of any defects in materials and workmanship under normal use and the Software will perform substantially in accordance with the Documentation. This limited warranty extends only to the original user of the Product. This limited warranty is void if failure of the Hardware or Software to conform to the warranty has resulted from improper installation, testing, misuse, neglect, accident, fire or other hazard, a virus, or any breach of this Agreement. Apposite and its suppliers' entire liability and your sole and exclusive remedy shall be, at Apposite's sole discretion, to: (i) repair the Software or Hardware; (ii) provide replacement Hardware or Software; or (iii) refund the purchase price and terminate this Agreement. This limited warranty applies only if the Product is returned to Apposite, freight and insurance prepaid, in accordance with Apposite's Return Material Authorization (RMA) procedures. Any repaired or replaced Software or Hardware will be subject to this same limited warranty for the remainder of the original Warranty Period or thirty (30) days, whichever is greater. THE FOREGOING LIMITED WARRANTY IS IN LIEU OF ALL OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, AND APPOSITE DISCLAIMS ANY AND ALL IMPLIED WARRANTIES OR CONDITIONS, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OF TITLE, NONINFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY BY JURISDICTION.

7. **LIMITATION OF LIABILITY.** REGARDLESS WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL APPOSITE OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES, INCLUDING WITHOUT LIMITATION, ANY LOST PROFITS, BUSINESS INTERRUPTION, LOSS OF INFORMATION, OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY OR WHETHER ARISING OUT OF THE USE OF OR INABILITY TO USE THE PRODUCT AND EVEN IF APPOSITE OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL APPOSITE OR ITS SUPPLIERS' LIABILITY, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), BREACH OF WARRANTY, OR OTHERWISE, EXCEED THE PRICE PAID FOR THE PRODUCT. SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION MAY NOT APPLY

TO YOU. YOU HEREBY WAIVE CALIFORNIA CIVIL CODE SECTION 1542, WHICH SAYS "A GENERAL RELEASE DOES NOT EXTEND TO CLAIMS WHICH THE CREDITOR DOES NOT KNOW OR SUSPECT TO EXIST IN HIS FAVOR AT THE TIME OF EXECUTING THE RELEASE, WHICH, IF KNOWN BY HIM MUST HAVE MATERIALLY AFFECTED HIS SETTLEMENT WITH THE DEBTOR."

- 8. TERM AND TERMINATION.** This Agreement takes effect upon your use of the Software and remains effective until terminated. You may terminate it at any time by destroying all copies of the Software and Documentation in your possession. The licenses granted by Apposite herein will terminate immediately if you fail to comply with any term or condition of this Agreement. You agree on termination of the licenses to cease all use of the Software and Documentation. In addition, the provisions of the sections "U.S. Government Restricted Rights" and "Export" shall survive termination of this Agreement.
- 9. EXPORT.** The Product, including the underlying technology, is subject to U.S. export control laws, and may be subject to export or import regulations in other countries. You may not export or import the Product and the underlying technology, directly or indirectly, in violation of these laws. You agree to comply strictly with all such laws and regulations and acknowledge that you have the responsibility to obtain such licenses to export, re-export, or import as may be required.
- 10. U.S. GOVERNMENT RESTRICTED RIGHTS.** All Software and Documentation provided pursuant to this Agreement qualifies as "commercial computer software" and "commercial computer software documentation" pursuant to FAR 12.212 and DFAR 227.7202. The Software and Documentation are being licensed to U.S. Government end users only as commercial items and with only those rights as are granted to all other end users pursuant to the terms and conditions of this agreement.
- 11. GENERAL PROVISIONS.** This Agreement will be governed by and construed in accordance with the laws of the State of California without reference to its conflicts of law provisions. Any dispute arising out of or relating to this Agreement shall be subject to the exclusive jurisdiction and venue of the courts sitting in Los Angeles, California. This Agreement shall not be governed by either the Uniform Computer Information Transactions Act (UCITA) or the United Nations Convention on Contracts for the International Sale of Goods (CISG), the application of which is expressly excluded. If for any reason a court of competent jurisdiction finds any provision of this Agreement, or any portion thereof, to be unenforceable, the remainder of this Agreement shall continue in full force and effect. This Agreement constitutes the entire agreement between the parties with respect to the Product and supersedes all prior or contemporaneous understandings regarding such subject matter, whether written or oral, and supersedes any conflicting or additional terms contained in any purchase order or elsewhere, all of which terms are excluded. No amendment to or modification of this Agreement are binding unless in writing and signed by Apposite.

Apposite® Technologies LLC

4223 Glencoe Ave, Suite B121

Marina Del Rey, CA 90292 USA

1.310.477.9955

info@apposite-tech.com

www.apposite-tech.com